TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 28 septembre 1999 (28.09.99)	
Demande internationale no PCT/FR99/00249	**Référence du dossier du déposant ou du mandataire** BCT990009 MF
Date du dépôt international (jour/mois/année) 05 février 1999 (05.02.99)	**Date de priorité** (jour/mois/année) 09 février 1998 (09.02.98)
Déposant CLERC, Fabrice etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

06 septembre 1999 (06.09.99)

[] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Diana Nissen

no de téléphone: (41-22) 338.83.38

Translation

09601933

21E1

2131

PT

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference BCT990009/ PL	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/FR99/00249	International filing date (*day/month/year*) 05 February 1999 (05.02.99)	Priority date (*day/month/year*) 09 February 1998 (09.02.98)
International Patent Classification (IPC) or national classification and IPC G07C 9/00		
Applicant LA POSTE		

RECEIVED
NOV 14 2000
TC 2700 MAIL ROOM

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
06 September 1999 (06.09.99)	10 April 2000 (10.04.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR99/00249

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1, 2, 4-21, 23-27, 29-37, as originally filed,
pages _____, filed with the demand,
pages 3,22,28, filed with the letter of 19 January 2000 (19.01.2000),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-11, filed with the letter of 19 January 2000 (19.01.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/6-6/6, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-10	**YES**
	Claims	11	**NO**
Inventive step (IS)	Claims	1-10	**YES**
	Claims	11	**NO**
Industrial applicability (IA)	Claims	1-11	**YES**
	Claims		**NO**

2. Citations and explanations

The subject matter of Claims 1-10 is novel and involves an inventive step as none of the documents cited describes or suggests the use of public key cryptography for key authentication by the lock. Documents EP-A-807 911 and EP-A-727 894, in this case, use a random secret session key or a secret communication key between the authority and the user respectively. The double use of cryptographic public key systems provides improved security.

Claim 11 is an independent claim since its subject matter is different from that of the other independent claims. This claim clearly indicates that it comprises cryptographic and transmission means for carrying out the protocol of one of Claims 1-17, but does not indicate the exact nature of these means in the preamble. Merely indicating means for carrying out a protocol which is the subject matter of an independent claim from another category does not have any limiting effect on said means.

Claim 11 specifies in the characterising portion, that these means comprise a memory zone storing a public key and a memory comprising the program for checking the signature. However, these means are already known from document FR-A-2 722 596.

Therefore the subject matter of Claim 11 is not novel.

I, John Richard Flood-Paddock, verify that the document attached as Exhibit A is a true and correct English-language translation of the text of International patent Application No. PCT/FR99/00249 attached as Exhibit B. I have been warned that wilful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001) and may jeopardize the validity of the application or any patent issuing thereon. All statements herein made of my own knowledge are true and all statements made on information and belief are believed by me to be true



John Richard Flood-Paddock

Dated this 25th day of July 2000

ACCESS CONTROL PROTOCOL BETWEEN AN ELECTRONIC KEY AND AN ELECTRONIC LOCK

The present invention relates to an access control protocol between an electronic key and an electronic lock effecting logical access control.

Logical control of access to buildings, to premises containing data processing systems or systems storing assets, fiduciary, technology or information assets, is currently of great and increasing interest.

Access control methods usually employ a portable access element functioning as a key, referred to as the accessing resource, and an access resource functioning as a lock.

Logical access control between an accessed resource functioning as an electronic lock and an accessing resource functioning as an electronic key currently consists of a succession of operations to verify information or messages exchanged between the electronic key and the electronic lock.

One of the main advantages of logical access control, compared to conventional physical access control of the lock-and-key type, is the facility to allow access to an accessed resource only within a predetermined short time period.

However, if the system comprising the accessing resource and the accessed resource provides one or several accessing resources allowing access to several accessed resources through similar logical access control, counterfeiting during the validity time period of either an electronic key functioning as the accessing resource or the access control dialogue between one of the electronic keys and one of the access resources functioning as an electronic lock can then allow illegitimate access to all of the accessed resources.

Merely reproducing the logical access control dialogue between the accessing resource and one of the accessed resources allows such illegitimate access through a procedure referred to as "playback".

A conventional solution that has been implemented with the aim of responding to any such illegitimate use applies logical access control based on cryptographic mechanisms to limit the period of validity of the right of access to a short period, to foil illegitimate use outside the validity time period in the event of loss, theft or illicit holding of the electronic key. One such solution, described in French Patent Application No. 2 722 596 (94 08770) in the name of FRANCE TELECOM and LA POSTE and published 9 January 1996, establishes a digital signature of the time period during which access is authorised. Access to the accessed resource is conditional on verification of the aforementioned digital signature within the accessed resource.

Another conventional solution implemented with the same aim, more particularly to respond to playback, uses a random variable to introduce a variability or diversity characteristic into the access control dialogue between the key and the electronic lock. A solution of this kind would appear to have limitations because the random nature of the random variables obtained by means of the usual random or pseudo-random generators is not totally satisfactory unless one or more external physical variables of a purely random nature are used and because non-repetitive production of such random numbers is not certain, and will therefore not discourage highly skilled hackers who are determined to succeed and who have access to powerful computation resources.

In any event, the aforementioned solutions are therefore unable to prevent with certainty either illegitimate use of an electronic key or playback during

the validity time period of an accessed resource.

The object of the present invention is to remedy the aforementioned drawbacks of prior art solutions.

An object of this kind is achieved in particular by integrating into the logical access dialogue between an accessing resource and at least one accessed resource a process of authentication of the accessing resource by the accessed resource and making authorisation or refusal of access conditional on a successful outcome of the authentication process.

Another object of the present invention is consequently to use an access control protocol between an accessing resource consisting of an electronic key and an accessed resource consisting of an electronic lock in such a way that the authentication process is conducted in accordance with a challenge-and-response protocol and, in a particularly remarkable manner, the risk of the electronic key being compromised is further and significantly reduced to that caused by the presence in the electronic key of a simple right of access.

A final object of the present invention is to prevent all risk of picking an electronic lock by playback in a given validity time period because of the very existence of the authentication process.

The access control protocol according to the invention between an electronic key and an electronic lock performing said access control is remarkable in that, following presentation of the electronic key to the electronic lock, the protocol consists of transmitting a random variable message prompting authentication of the electronic key from the electronic lock to the electronic key. On receiving the random variable message prompting authentication, a signature value of the random variable message prompting authentication and specific authentication data are transmitted from the electronic

key to the electronic lock, the signature value transmitted being calculated from a private signature key and the specific authentication data. After reception by the electronic lock of the signature value and the specific authentication data, the electronic lock verifies the authenticity of the signature value as a function of the specific authentication data. In response to a positive or negative result of said verification access is accepted or respectively refused.

The access control protocol in accordance with the invention between an electronic key and an electronic lock can be applied to all types of accessing resource and to all types of accessed resource.

Because the risk of playback is eliminated, calculating the signature value of the random variable message prompting authentication, making determination of that signature improbable in the absence of physical possession of the electronic key generating it, the protocol according to the present invention would appear to be particularly well suited to the secure management of a plurality of accessed resources, such as mailboxes, or even strongboxes, by means of one or more accessing resources, or electronic keys, enabling legitimate access to each of the accessed resources, the number of electronic keys being very much less than the number of mailboxes or strongboxes.

The invention will be better understood after reading the following description and referring to the accompanying drawings, in which:

- figure 1a shows a general block diagram of the access control protocol in accordance with the present invention between an electronic key and an electronic lock;
- figure 1b shows a sequential flowchart of the succession of steps for implementing the access control

protocol in accordance with the present invention between an electronic key and an electronic lock;

- figure 1c shows a preferred embodiment of a signature verification procedure used by an electronic lock (accessed resource) in accordance with the protocol according to the present invention;

- figure 1d shows one example of a mode of operation for obtaining a random variable message providing an authentication process in accordance with the protocol according to the present invention;

- figure 1e shows a procedure carried out by an electronic key for auxiliary verification of a public key enabling the electronic key to perform the random variable message signature operation in the context of the protocol according to the present invention;

- figure 1f shows one example of a method of reducing picking of an electronic lock outside at least one validity time period conforming to the protocol according to the present invention;

- figure 1g shows a particularly advantageous variant of the auxiliary verification process shown in figure 1e in which, if the electronic key has an internal clock, an additional security feature consisting of total invalidation of the electronic key is provided for situations in which access is attempted outside the validity time period;

- figure 2a shows a first advantageous variant of the protocol according to the present invention which avoids storing a second public key in each electronic lock, which increases the overall security level of the system as a whole;

- figure 2b shows a sequential flowchart of the steps of the protocol shown in figure 2a;

- figure 3a shows a block diagram of the electronic architecture of an electronic key for

implementing the access control protocol according to the present invention; and

- figure 3b shows a block diagram of the electronic architecture of an electronic lock for implementing the access control protocol according to the present invention.

An access control protocol in accordance with the present invention between an electronic key and an electronic lock providing logical access control will now be described in more detail with reference to figures 1a and 1b.

The access control protocol according to the present invention consists of a logical access control dialogue between the electronic key and at least one electronic lock, this logical access control incorporating a process of authentication of the electronic key by the electronic lock in order to authorise or refuse access. The authentication process uses message and/or data signature calculation and signature verification operations verifying the authenticity of the aforementioned messages or data.

By way of non-limiting example, the signature calculation operations followed by the signature verification operations included in the protocol according to the present invention can be based either on a secret key signature algorithm or on a public key algorithm using a private signature key associated with a public signature verification key.

The signature calculation and signature verification operations for implementing the access control method according to the present invention are described hereinafter in connection with one non-limiting preferred embodiment of the invention using an encryption or signature algorithm employing at least one public key and one private key, the algorithm being the RSA algorithm

developed by RIVEST, SHAMIR and ADLEMAN, for example. Other public key algorithms can be used without disadvantage.

Employing the usual terminology, in the context of the signature calculation and signature verification processes, if a public key algorithm is used, any signature key is a private key, which must be kept secret, whereas any signature verification key is a public key, which can be divulged. However, if a secret key algorithm is used and the secret key can be used as an encryption key to carry out a signature operation, a key of this kind and the signature verification key must be secret keys.

By convention, for any private key used to calculate a signature, the notation used for the calculation of the signature obtained by application of the private key K_S by the signature algorithm used, i.e. the RSA algorithm in the context of this example, is:

$S_{KS}(A,B,C)$

Likewise, the notation used for any signature verification operation effected by applying the public key K_P associated with the private key K_S to the aforementioned signatures or signed messages X,Y,Z, the signature being a digital message, is:

$\nu_{KP}(X,Y,Z)$

In any signature calculation operation, respectively signature verification operation, A,B,C, respectively X,Y,Z, designates the arguments subjected to the signature operation, respectively signature verification operation, these arguments consisting of messages or data, of course, as previously mentioned.

By definition, the verification operation using the public key K_P applied to a signature obtained by means of a private key K_S applied to an argument A and taking A as an input parameter produces a Yes/No verification

response. This verification is written:

- $v_{KP}(S_{KS}(A),A)$ = Yes/No.

If message re-establishing algorithms are used for the signature and signature verification operations, such as the RSA algorithm, a verified value VA of the argument A is obtained, and is supposedly equal to the argument A itself, of course.

To be more specific, to enable the use of the access control protocol according to the present invention, the electronic key and the electronic lock are each provided with modules Ca_k and Ca_i for calculating and memorising data, to enable storage in memory of any message necessary for the identification process, calculation of the signatures and verification of the signatures to enable use of the authentication process. The suffixes k and i represent a physical reference or address allocated to an electronic key and to an electronic lock, respectively.

In figure 1a and the subsequent figures, an electronic key EK_{kj} is used to implement the access control protocol according to the invention. The suffix k corresponds to a serial number or identifying number of the electronic key itself. The suffix j corresponds to a validation operation reference or address for the electronic key EK_{kj}, as described in more detail later. Each electronic key EK_{kj} is therefore provided with a calculation module Ca_k and a message transmission module T_k, represented by a wire antenna connected to the calculation unit Ca_k, the wire antenna enabling transmission of messages by electromagnetic means, for example.

The same applies to each electronic lock. Figure 1a shows a set of electronic locks B_1, B_i to B_N, each electronic lock B_i having a calculation and memory module Ca_i and a transmission module T_i represented by a wire

antenna and enabling electromagnetic transmission and reception of messages or data, for example.

In the event of an attempt to access a lock B_i using a key EK_{kj}, the respective wire antennas T_k and T_i are brought face-to-face to enable the exchange of messages for assuring the previously mentioned logical access control.

Generally speaking, in figure 1a, as in all the figures accompanying this description, in any general block diagram including various actors of the access control protocol according to the invention, any transaction, i.e. any exchange of messages between actors, is represented by an arrow extending from one of the actors to the other.

If an operation is effected internally, by the actors, that operation is represented by a closed arrow indicating internal execution for the actor concerned.

Finally, any transaction between two actors performed as an antecedent to implementation of the protocol according to the present invention is represented by a dashed line arrow.

The access control protocol according to the present invention between an electronic key and an electronic lock is implemented under the control of a certification authority shown diagrammatically in figure 1a and responsible for general management of the set of electronic keys EK_{kj} and the set of electronic locks B_i accessible by means of at least one of the electronic keys.

As shown in figure 1a, the certification authority can consist of a signature entity which is approved to choose and define a private key K_s in the context of execution of the signature algorithms previously referred to. The private signature key K_s is therefore chosen by the signature entity and this signature key is neither

communicated nor divulged to any other actor authorised to use the access control protocol according to the present invention.

The certification authority further comprises a validation entity which can be separate from the signature entity but is related to it hierarchically. The signature entity communicates to the validation entity the public key K_P associated with the private key K_S and authentication data DA_j which in fact consists of the signature using the private key K_S held by the certification authority of a certain number of arguments, including in particular a second public key K'_P, a time period value PH_j associated with the second public key K'_P and, for example, specific auxiliary data AUX. In the remainder of the description, the time period PH_j is referred to as the validity time period.

The second public key K'_P is associated with a private key K'_S. The initiative for choosing the second private key K'_S and the second public key K'_P can be accorded to the validation entity.

To implement the access control protocol according to the present invention, each electronic key EK_{kj} is subjected to a validation operation V_j consisting of loading and/or downloading the data parameters and messages held by the validation entity and needed to implement the access control protocol according to the present invention into the memory circuits of each of the aforementioned electronic keys EK_{kj}. The operation V_j is therefore shown in chain-dotted line in figure 1a, because it is carried out before the first use of a particular electronic key, of course. During this operation, the authentication data DA_j and the second private key K'_S are loaded into the memory circuits of each electronic key EK_{kj} and appropriate memory circuits for the data and the key are preferably provided in the

calculation unit Ca_k, the memory circuits including at least one protected memory area whose level of protection substantially corresponds to that of the protected memory areas of a smart card, for example, in order to store the second private key K'_s in a secure manner. The authentication data DA_j is specifically loaded before one or more uses of the electronic key EK_{kj}.

Thus each electronic key EK_{kj}, which is unusable before any validation operation V_j, is in fact replaced by an operational electronic key EK_{kj}, the suffix j designating the reference to the authentication data DA_j associated with the aforementioned electronic key, and in particular the validity time period of the second private key K'_s and the second public key K'_p associated with that time period.

Also, the validation operation V_j consists of loading or downloading into each key EK_{kj} the first public key K_p corresponding to the first private key K_s held by the certification authority. Specifically, the first public key K_p is loaded once only into each electronic key EK_{kj} before one or more successive uses, according to the key management policy defined by the certification authority for each application concerned.

A step V_i (figure 1a) of validating each electronic lock B_i consists of storing in memory and loading and/or downloading into the memory circuits of each calculation unit Ca_i the first and second public keys K_p, K'_p referred to previously.

After the aforementioned validation operations V_j and V_i, the access control protocol according to the present invention can be conducted between a validated electronic key EK_{kj} and any electronic lock B_i that has also been validated, as previously mentioned.

Any attempt at access by an employee holding an electronic key EK_{kj} entails that person bringing together

the respective transmission units T_k and T_i of the electronic key and the electronic lock.

This having been effected (by way of non-limiting example) between the key and the lock B_i shown in figure 1a, the electronic key EK_{kj} sends the electronic lock B_i an identification request message A_{ki}. The identification request message can be an identification number specific to the electronic key EK_{kj}, for example. Following verification of the identification request message A_{ki}, the electronic lock B_i can implement the access control protocol according to the present invention, as described hereinafter. The aforementioned verification operation can simply consist of verifying the value of the message communicated against reference values.

Referring to the aforementioned figure, the access control protocol according to the present invention consists at least of transmission from the electronic lock B_i to the electronic key EK_{kj} of a random variable message a_{ij} prompting authentication of the electronic key, after reception by the electronic lock B_i of the identification request message A_{ki} sent to it by the accessing electronic key.

Following reception by the electronic key of the random variable message a_{ij} prompting authentication, the key calculates a signature value C_i of the random variable message prompting authentication. In figure 1a, this step is denoted:

$$C_i = S_{K's}(a_{ij}).$$

Given the convention indicated, the signature value of the random variable message prompting authentication is obviously obtained from the second private key K'_s. It is clear in particular that the signature operation C_i in respect of the random variable message prompting authentication a_{ij} in fact establishes the right of access of the electronic key to the electronic lock for the true

value of that signature. It is further clear, in accordance with one particularly advantageous aspect of the protocol according to the present invention, that the right of access is modified for each transaction and each attempted access.

Following this signature calculation step, the electronic key EK_{kj} transmits to the electronic lock B_i the signature C_i and specific authentication data DA_j, the data being specific to the validity time period PH_j of the second private key K'_s and the second public key K'_p associated with that validity time period, of course. The aforementioned transmission operation is denoted C_i, DA_j in figure 1a.

Following reception by the electronic lock B_i of the signature value C_i and the specific authentication data DA_j, the electronic lock B_i verifies the authenticity of the signature value as a function of the specific authentication data, as shown by a closed arrow in figure 1a. In the same manner as previously, the aforementioned verification operation by the electronic lock B_i is denoted $v_{KPK'P}((C_i,DA_j),K_p,K'_p)$ = Yes/No.
Given the convention previously adopted, it is clear that the aforementioned verification step is effected by applying the first and second public keys K_p, K'_p, taken as parameters. The application of the aforementioned keys can also restore verified values of the random variable message transmitted by the electronic lock B_i to the electronic key and the specific authentication data DA_j. The verification operation enables the electronic lock B_i to decide to accept or refuse the requested access, according to whether they are authentic or not. Thus in the event of a positive result (Yes) of the aforementioned verification step, access is allowed whereas in the event of a negative result (No) access is refused.

A sequential description of the access control protocol according to the invention, as shown by the general block diagram in figure 1a, will now be given with reference to figure 1b.

In figure 1b, step 1000 represents the step of transmission by the electronic key EK_{kj} of the identification request message A_{ki}. That step is followed by a step 1001 representing the transmission of the random variable message a_{ij} by the electronic lock B_i to the electronic key EK_{kj}. The next step 1002 represents, based on the initial validation data V_j, and successively, the calculation of the random variable message signature C_I and transmission of the signature and the specific authentication data DA_j. The preceding step 1002 is itself followed by the step 1003, effected by the electronic lock and based on the initial validation data V_i, of verifying the authenticity of the signature value, according to the specific authentication data.

By way of non-limiting example, and for simplicity, the aforementioned verification step can generate a verification variable V, itself corresponding to a logic value 0 or 1, i.e. to the Yes or No result mentioned previously. This being the case, step 1003 is then followed by a step 1004 which is carried out at the level of the electronic lock to verify the true value of the verification logic variable V or the Yes, No result. The true value of the latter leads to authorisation of access (step 1006) whereas the absence of a true value leads to refusal of access (step 1005).

With regard to the nature of the specific authentication data DA_j transmitted by the electronic key EK_{kj} to the electronic lock B_i, as shown in figure 1a, the data consists of at least a public key certificate associated with the private signature key K'_s. The public key certificate consists of a digital signal value of at

least one validity time period PH_j relative to a right of access and the second public key K'_P.

Accordingly, given the convention previously indicated, the specific authentication data DA_j corresponds to the signature S_{KS} of various arguments such as the second public key K'_P associated with the private signature key K'_S, at least one time period PH_J associated with the second public key K'_P, the specific authentication data Da_j being obtained by application of the private signature key K_S of the signature entity. In particular, it is clear for example that various time period values can be used, for example by employing a diversity program for choosing a specific time period from among several such periods.

Note, however, that apart from the two second public key arguments K'_P and PH_j previously mentioned, another argument relating to the auxiliary data AUX can be subjected to the aforementioned signature operation S_{KS}. The auxiliary data can advantageously comprise, although this is not limiting on the invention, a serial number of the associated electronic key EK_{kj}, that serial number representing a code of the suffix k indicative of the aforementioned electronic key. Other digital values or data can be transmitted by the electronic key, by way of the field relating to the auxiliary data, as described later.

The transmission steps 1000, 1001 and the transmission substep of step 1002, as shown in figure 1b, are performed by the transmission systems of the electronic key EK_{kj} and the lock B_i, denoted by the reference T_i in the case of the lock.

Finally, in one advantageous embodiment of the access control protocol according to the present invention, the step of transmitting the electronic key EK_{kj} to the electronic lock B_i, shown in figure 1a and

referenced 1002 in figure 1b, can consist of transmitting the second public key K'_P obtained from the authentication data DA_j, for example, in addition to the signature value C_i of the random variable message prompting authentication and the authentication data DA_j. For this reason, the second public key K'_P is shown in parentheses during the transmission step shown in figure 1a and referenced 1002 in figure 1b. In a case like this, it is naturally not necessary to store the second public key K'_P in memory in the electronic lock during the operation V_i to validate each electronic lock B_i. The first public key K_P is then used during the operation of verifying the authentication data $v_{KPK'P}$ (C_i, DA_j) to attest to the authenticity of the second public key K'_P transmitted.

Generally speaking, the step of verification of the authenticity of the signature value by the electronic lock can be effected by means of a secret key when the signature calculation operation is based on that secret key or another secret key or a public key if the signature operation is based on a private key.

A more detailed description of the verification step 1003 effected by the electronic block B_i will now be given with reference to figure 1c, in the specific but non-limiting situation of using a message re-establishing algorithm such as the RSA algorithm.

As shown in the aforementioned figure, the verification step 1003 includes, in succession, a first verification step 1003a effected by the electronic lock B_i, this verification consisting of verifying the authenticity of the specific authentication data DA_j against reference data comparison criteria stored previously in the memory circuits of the electronic key EK_{kj}. It is clear in particular that applying the first public key K_P available to the signature S_{KS} provides a verified value of the public key K'_P associated with the

private signature key K'_S, given the conventions referred to above, the verified public key value denoted VK'_P, and a verified value of the time period PH_j. The auxiliary data is also reproduced when auxiliary data is transmitted by means of the argument AUX in the signature S_{KS}.

Accordingly, and in a manner that is not limiting on the invention, the reference data stored in the memory circuits of the electronic key EK_{kj} does not correspond only to the second public key K'_P associated with the private signature key K'_S, the time period value PH_j and, where applicable, the serial number of the key, which can be stored in a protect read-only circuit. The verified values following the operation of verifying the reference values can then be compared by a simple equality comparison 1003a. In step 1003a there is merely shown the equality test on the verified value of the second public key VK'_P against the stored value of the second public key K'_P.

In the event of a positive result of the aforementioned comparison in step 1003a, a second verification is performed by the electronic lock B_i in step 1003b. As shown in the aforementioned figure, this second verification consists of verifying the signature value of the random variable message prompting authentication.

Given the previous conventions, the second verification is denoted:

$$v_{K'P}(C_i) = v_{K'P}(S_{K'S}(a_{ij})).$$

Clearly during this second verification step performed in step 3000b, a verified value Va_{ij} is obtained for the random variable message prompting authentication. The verified value of the random variable message prompting authentication can then be compared with the random variable message prompting authentication a_{ij}, which will

have been stored beforehand in the memory circuits of the electronic block B_i, of course.

Thus it is clear that the second verification of the signature value is conditional on verification of the second public key K'_P associated with the private signature key K'_S and therefore, in the final analysis, on the aforementioned specific authentication data DA_j.

Generally speaking, the first verification of the authenticity of the specific authentication data, represented in step 1003a in figure 1c, can consist of checking the validity time period PH_j associated with the second public key K'_P. By applying the first public key K_P to the signature $S_{KS}(K'_P, PH_j, AUX)$, the verification step v_{KP} enables the value of the validity time period PH_j associated with the second public key K'_P to be obtained, alone, of course.

As shown in figure 1d, the random variable message prompting authentication a_{ij} mentioned above can depend on an identification value CB_i of the electronic lock. It can correspond to a serial number or a coded arbitrary number allocated to the aforementioned electronic lock B_i.

As also shown in figure 1d, the random variable message a_{ij} can also depend on a continuously increasing variable count value CO which can correspond to a date value expressed as a year Y, month M, day D, hour H, minute m and second s.

It is clear, for example, that the field CB_i and the field CO relating to the identification value of the electronic lock and to the continuously increasing variable value can be coded on the same number of bits, for example 32 or more bits, in which case each field can be combined bit-by-bit on the basis of a logical composition law $\otimes$, for example, to generate a component r_{ij} of the random variable message prompting authentication, as shown in figure 1d. The composition

law is an exclusive-OR operation, for example. The random variable message a_{ij} is then obtained by concatenating the component r_{ij} and the fields CB_i and CO. This coding method guarantees that the random variable message obtained is not repetitive.

Although the field relating to the serial number of the electronic lock CB_i can be given by any protected memory element available in the memory circuits of the aforementioned electronic lock, the count value CO can be delivered either by an incremental counter or by an internal clock available in each electronic lock. Using an incremental counter has the advantage of simplifying the circuits required to implement each electronic lock.

One particularly advantageous embodiment of the access control protocol according to the present invention between an electronic key and an electronic lock will now be described with reference to figure 1e.

Figure 1e shows the electronic key EK_{kj} as shown in figure 1a, for example. However, in addition to the calculation circuits Ca_k associated with the aforementioned electronic key, the key has an internal clock CK. The internal clock delivers a clock signal VCK to the corresponding calculation unit Ca_k.

This being so, and as shown in figure 1e, the protocol according to the present invention further consists of an auxiliary verification step 1007 for verifying authorisation of signature calculation for the random variable message prompting authentication. The auxiliary verification step is carried out by the electronic key EK_{kj} following reception of the random variable message prompting authentication a_{ij} in step 1001, as shown in figure 1a, but before the step of calculation and transmission of a signature value by the electronic key, as shown in step 1002 in the aforementioned figure.

The auxiliary verification step 1007 consists of using the first public key K_P to check the public key certificate and the validity time period PH_j associated with the aforementioned second public key K'_P against the internal clock.

Given the above conventions, and taking the second public key K'_P as a parameter, the verification operation is denoted:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX), K'_P)$ = Yes/No

However, using a message re-establishment algorithm leads to an operation denoted:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX))$

which produces the verified value VK'_P of the second public key which can be compared to the value of the second public key K'_P, as previously mentioned.

The aforementioned verification step then provides the verified value of the validity time period PH_j. The value of the clock signal VCK is compared to the validity time period PH_j to verify the validity of the second public key K'_P with which the aforementioned validity time period is associated. For example, the value of the clock signal VCK for a given validity time period can be compared to the limits which define the aforementioned validity time period PH_j.

Step 1007a is followed by a step 1007b consisting of verifying the association of the second private signature key K'_S with the second public key K'_P whose validity was verified in the preceding step 1007a. The association verification operation carried out in step 1007b can consist of calculating a signature $S_{K'S}(X)$ obtained by applying the second private signature key K'_S to a random variable X generated by the electronic key EK_{kj} (see figure 1e). A verification step applied to the verification signature value ($S_{K'S}(X)$ then constitutes the association verification step, the verification applying

to the signature calculated previously and being denoted:

$v_{K'P}(S_{K'S}(X))$.

This verification step produces a verified value VX of the random variable X in step 1007b. A test which compares the verified value VX of the random variable X with the previously stored random variable X determines the validity of the association of the second private signature key K'_S with the second public key K'_P, whose validity was verified in the preceding step 1007a.

Verifying that the validity time period PH_j is compatible with the clock signal VCK, that the verified value VK'_P of the second public key K'_P is identical to the value of the second public key K'_P, and that the verified value of the random variable VX is identical to the value of the random variable X constitutes a test which, if the result is positive (step 1007c, see figure 1e), enables the protocol according to the present invention to continue (step 1007e), which is followed by the signature of the random variable message prompting authentication a_{ij} (step 1002). In the event of a negative result, the aforementioned protocol is interrupted (step 1007d).

Performing the verification operations 1007a and 1007b using the message re-establishment signature verification algorithms, such as the RSA algorithm, previously referred to can preferably be carried out when the second public key K'_P is transmitted, in the subsequent step of transmitting the electronic key EK_{kj} to the electronic lock B_i. In any other case, in the absence of such transmission, the verification operation can be reduced to an operation of the following type, taking the second public key K'_P as parameter:

- $v_{KP}(S_{KS}(K'_P, PH_j, AUX), K'_P)$ = Yes/No

What is more, the protocol according to the present invention can be adapted to limit all attack outside of

the validity time period PH_j associated with the second public key K'_P.

To this end, as shown in figure 1f, during the step of verification by the electronic lock B_i of the authenticity of the signature value (step 1003 in figure 1a and more particularly steps 1003a and 1003b in figure 1c), following the first step 1003a of verifying the authenticity of the specific authentication data DA_j, consisting of checking the validity time period associated with the first public key K_P, but prior to the second verification step 1003b shown in figure 1c, a plurality of tests ($1003a_1$, figure 1f) can be carried out to limit all attack outside the aforementioned validity time period. In figure 1f, the plurality of tests is represented, in a manner that is not limiting on the invention, as a comparison, within the aforementioned validity time period, of the count value CO delivered by the electronic lock B_i or, where applicable, a time signal delivered by a clock when the electronic lock has a clock. To be more specific, this test can consist of comparing the count value CO to limits defining the aforementioned validity time period PH_j, for example. If the count variable CO or the corresponding time signal is not inside the validity time period, the electronic lock B_i refuses any attempt at access. Other tests limiting attack outside the validity time period can be considered.

With regard to tests for limiting all attack outside a particular time period PH_j, a preferred non-limiting embodiment will be described hereinafter in the situation where the electronic key has a real-time clock. At the time of any attempt at access, if the verification step such as the step 1007a has been effected validly at the level of the electronic key EK_{kj}, in particular the test for the compatibility of the time variable delivered by

the clock signal VCK with the time period PH_j, the current time variable VCK delivered by the real time clock is stored in the electronic key EK_{kj}.

During the step of transmitting the electronic key EK_{kj} to the electronic lock B_i, shown in Fig.1a and referenced 1002 in Fig.1b, the time variable VCK is transmitted in addition to the signature value C_i and the authentication data DA_j, and the second public key K'_p where applicable. For this reason the time variable is shown in brackets.

The subsequent verification steps can then be performed in the electronic lock B_i.

As shown in figure 1f, for a count value CO delivered by a counter in the electronic lock B_i, a count value at the time of the attempt at access and a reference value VC_{ref} corresponding to a count value at the time of a previous attempt at access, for example, are stored in the lock.

For a time period PH_j reduced to a time interval $[VH_1, VH_2]$, it is verified that the time variable VCK stored in memory and transmitted is after VH_1 and before VH_2 and also that VCK is after VC_{ref}. If any of the foregoing verifications is not satisfied, access to the lock B_i is barred. It is accepted otherwise.

Of course, and in a manner that is not limiting on the invention, the time period PH_j can comprise a plurality of non-contiguous time intervals. In this case, the time period PH_j can be expressed in the form of a union of time intervals, in which U represents the UNION operator:

$$PH_j = [VH_1, VH_2] \cup [VH_3, VH_4] \cup \ldots \cup [VH_{n-1}, VH_n]$$

The limits which delimit each time interval can advantageously each be expressed as a date in the form day, month, year and a time in the form hour, minute, second.

To confer a very high level of security on the access control protocol according to the present invention, even more strict measures can be applied, in particular at the level of the electronic key EK_{kj}, to limit further risk of fraudulent use of the electronic key, in particular if it is lost or stolen. To this end, as shown in figure 1g, the step 1002 shown in figure 1a of calculating a signature value of the random variable message prompting authentication can be preceded by a signature authorisation auxiliary verification step, repeating some parts of the verification step 1007 shown in figure 1e, but increasing the security level of the verification by introducing a step of self-invalidation of the electronic key EK_{kj} under conditions explained below.

The electronic key EK_{kj} includes a clock CK delivering a clock signal VCK required for implementing the auxiliary verification step shown in figure 1g, in the same manner as in the case of implementing the auxiliary verification step of figure 1e.

This being so, as shown in figure 1g, the auxiliary verification step 1007 comprises a step of checking that a time variable, the clock signal VCK delivered by the real time clock CK, is inside the validity time period PH_j. Clearly, to this end, the step 1007a shown in figure 1g corresponds substantially to the step 1007a shown in figure 1e.

Likewise the step 1007b shown in both of the aforementioned figures.

In the case of figure 1g, the step 1007c of figure 1e is in fact subdivided into two sub-steps $1007c_1$ and $1007c_2$, for example.

The step $1007c_1$ consists of testing that the time variable VCK delivered by the real-time clock is inside the validity time period PH_j. If the result of the test in

step $1007c_1$ is positive, step $1007c_2$ compares the verified value VK'_P of the second public key K'_P to the value of the second public key K'_P and the verified value VX of the random variable X to the aforementioned random variable X, for example.

If the result of the test in step $1007c_1$ is negative, for example, in other words if the time variable VCK is not inside the time period PH_j, the protocol according to the present invention consists of executing a step $1007c_3$ which invalidates the electronic key EK_{kj}. The invalidation step $1007c_3$ then leads, of course, to a step 1007d of interrupting the access control protocol according to the present invention, on the grounds that the electronic key cannot be used.

Various techniques can be used to invalidate the electronic key EK_{kj}, such as short-circuiting the supply voltage of the electronic circuits, i.e. the calculation circuit Ca_k of the electronic key, and dissipating all of the electrical energy powering those circuits, or where applicable setting one or more switch-off variables for inhibiting the operation of the electronic key concerned.

On the other hand, if the result of the test in step $1007c_2$ shown in figure 1g is positive, the protocol continues (step 1007e, i.e. step 1002 of calculating the signature of the random variable prompting authentication a_{ij} as shown in figure 1a).

Variants of the access control protocol according to the present invention are naturally feasible, in particular to assure an optimum level of security, both at the level of each electronic key EK_{kj} and at the level of each electronic lock B_i.

Figure 2a shows a variant of the access control protocol according to the present invention which is particularly noteworthy in that no second public key K'_P is stored in memory in each electronic lock B_i.

To this end, firstly, the operation of validating each electronic lock B_i consists of a validation operation V_i in which only the first public key K_p is stored in the memories of the calculation units of each electronic lock B_i.

Secondly, the operation V_j of validating each electronic key EK_{kj} consists of transmitting only the specific authentication data DA_J and the second private signature key K'_s. The second private signature key K'_s is transmitted and stored in the memories of the calculation circuits Ca_k of the electronic key EK_{kj}.

During attempted access, in accordance with the protocol according to the present invention, the steps of transmitting the access request identification message A_{ki} and the random variable message prompting authentication a_{ij} from the electronic lock B_i to the electronic key EK_{kj} are unchanged.

On the other hand, the step 1002 previously described of calculating the signature value of the random variable message prompting authentication a_{ij} is modified in the following manner. The authentication data is verified first, this verification being denoted $v_{KP}(S_{KS}(K'_P, PH_j, AUX))$.

With the preceding convention, the second public key K'_P is restored, which enables the signature value $C_i = S_{K'S}(a_{ij})$ of the random variable message to be calculated on the basis of the available second private signature key K'_s. Because the signature value is available and stored in memory, the operation of transmitting the signature C_i of the random variable message prompting authentication, the specific authentication data DA_j and the second public key K'_P to the lock B_i can be carried out.

The protocol according to the present invention is then resumed at step 1003 of figure 1a for example by the

lock B_i.

All the verification steps, followed by the steps of calculating the signature values C_i, followed by the aforementioned transmission, are represented in steps 1002a, 1002b, 1002c of figure 2b, prior to execution of the step 1003 previously mentioned.

There follows a description with reference to Figures 3a and 3b of the architecture of an electronic key and an electronic lock for implementing the access control protocol according to the present invention.

Figure 3a shows an electronic key EK_{kj} which has a cryptographic calculation module Ca_k, a message or data transmission module E_k and a transmit/receive wire antenna T_k, as previously described. The cryptographic calculation module comprises, in addition to a central processor unit CPU, a protected access memory area 1 for storing at least one signature value of a validity time period allocated to the electronic key, that signature value corresponding of course to the specific authentication data DA_j previously mentioned. The protected access memory area 1 is also used to store a signature verification key, the first public key K_p, i.e. the aforementioned signature, consisting of the specific authentication data. It also stores a signature key, the second signature key K'_s mentioned previously. This embodiment corresponds to the embodiment of the protocol according to the present invention shown in figure 1a.

The cryptographic calculation model Ca_k also includes a read-only memory (ROM) 2 enabling the central processor unit CPU to call programs for calculating the signature value of a random variable message, i.e. the message a_{ij} previously mentioned, and for signature verification on the basis of the signature keys, respectively signature verification keys, i.e. the keys K'_s and K_p previously mentioned. The read-only memory 2 of

the key stores programs for calculating signature values of the random variable message and verifying signatures on the basis of the signature keys K'_s and signature verification keys K_p, K'_p, as in the flowcharts shown in figures 1e and 1g previously described.

In addition to the above, and depending on the embodiment of the protocol according to the present invention used, the cryptographic calculation module Ca_k includes a clock 3, for example, delivering the clock signal VCK to the central processor unit CPU and, of course, a scratchpad random access memory (RAM) 4.

Finally, the system has a serial port PS for implementing the validation step V_j previously mentioned.

With regard to the electronic lock B_i shown in figure 3b, it has, of course, a cryptographic calculation module Ca_i and a message transmission/reception module E_i both associated with an antenna T_i which is shown as a wire antenna in figure 3b, without this being limiting on the invention.

The cryptographic calculation module Ca_i includes a protected access memory area in addition to a central processor unit CPU. The protected access memory area is used to store at least one public signature verification key, i.e. the first public key K_p and the second public key K'_p in the embodiment of the protocol according to the present invention shown in figure 1a, or respectively to store a single public key, i.e. the first public key K'_p in the embodiment of the protocol according to the present invention shown in figures 2a and 2b.

What is more, a read-only memory 6 connected to the central processor unit enables the central processor unit to call signature verification programs based on the public key or keys K_p, K'_p previously mentioned. The read-only memory 6 stores signature verification programs, for example, whose flowchart corresponds to that shown in

figures 1d, 1c and 1f previously described. Similarly, a counter 7 or if necessary a real-time clock and a serial port PS are provided.

An access control protocol between an electronic key and an electronic lock has therefore been described, the electronic lock applying access control in a particularly powerful manner in that the electronic key, which has cryptographic potential, is able to authenticate its attempt to access each of the accessed electronic locks.

A protocol of the above kind would appear to be of major benefit because the operation of signature by the key of the random variable message prompting authentication constitutes a variable right of access, changing on each transaction, so that playback is prevented.

Finally, the protocol according to the present invention can be used to optimise the overall security level in that a single signature verification public key can be stored in each electronic lock. It constitutes a secure method of access control. The optimisation is adapted to suit the application.

The protocol according to the present invention and the electronic key and the electronic lock for implementing the protocol would appear to be particularly suitable for management by approved employees of strongboxes or mailboxes, for example.

CLAIMS

1. An access control protocol between an electronic key and an electronic lock performing access control, in which protocol, following presentation of said electronic key to said electronic lock, a random variable message prompting authentication of the electronic key is transmitted from said electronic lock to said electronic key, characterised in that, on receiving said random variable message prompting authentication, the protocol consists of at least, in succession:

- calculating and transmitting from said electronic key to said electronic lock a signature value of said random variable message prompting authentication and specific authentication data, said specific authentication data transmitted by said electronic key to said electronic lock consisting of at least one public key certificate associated with said private signature key, said public key certificate consisting of a digital signature value of at least one validity time period relating to a right of access and of said public key, said signature value being calculated from a private signature key and the specific authentication data, and, after reception by said electronic lock of said signature value and said specific authentication data:

- verification by said electronic lock of the authenticity of said signature value as a function of said specific authentication data and, in response to a positive or negative result of said verification:

- acceptance or respectively refusal of said access.

2. A protocol according to claim 1, characterised in that the step of verification by the electronic lock of the authenticity of the signature value uses a secrete key or a public key.

3. A protocol according to claim 1, characterised

in that said step of verification of said signature value by said electronic lock includes, in succession:

- verification by said electronic lock of the authenticity of said specific authentication data based on comparison with reference data and, in the event of a positive result of said comparison:

- verification by said electronic lock of said signature value as a function of said specific authentication data.

4. A protocol according to claims 1 and 3, characterised in that said step of verification by said electronic lock of the authenticity of said specific authentication data consists of checking said validity time period associated with said public key.

5. A protocol according to claim 3, characterised in that validity time period includes a plurality of non-contiguous time intervals.

6. A protocol according to claim 3 or claim 4, characterised in that each validity time period consists of at least one time interval having two limits each expressed as a date in terms of day, month, year and a time in terms of hour, minute, second.

7. A protocol according to any preceding claim, characterised in that said random variable message prompting authentication is a function of an identification value of said electronic lock and a continuously increasing variable value.

8. A protocol according to any of claims 1 to 7, characterised in that, after reception of said random variable message prompting authentication by said electronic key but before the step of calculation and transmission of a signature value by said electronic key, said electronic key having an internal clock, said protocol further consists of an auxiliary verification step for authorising calculation of the signature of said

random variable message prompting authentication, said auxiliary verification step consisting of:

- using said public key to verify said public key certificate and said validity time period associated with said public key against said internal clock, to verify the validity of said public key,

- verifying the association of said private signature key and said public key, whose validity has been verified in the preceding step, and, on the basis of positive and negative result criteria for the preceding two verification steps:

- continuing or respectively interrupting said access control protocol.

9. A protocol according to any of claims 3 to 8, characterised in that it further comprises a plurality of tests limiting all attack outside said validity time period, which tests are performed during said step of verification by said electronic lock of the authenticity of said signature value, after said step of verification by said electronic lock of the authenticity of the specific authentication data consisting of checking said validity time period associated with said public key but before said step of verification by said electronic lock of the authenticity of said signature value said protocol further comprising a plurality of tests limiting any attack outside said validity time period.

10. A protocol according to any of claims 1 to 9, characterised in that it comprises, before said step of calculation and transmission from said electronic key to said electronic lock of a signature value of said random variable message prompting authentication and specific authentication data, said electronic key including a real-time clock:

- a step of testing if a time variable delivered by said real-time clock is inside said validity time period

and, in the event of a negative result of said test:

- a step of invalidation of said electronic key interrupting said access control and leading to refusal of said access by said electronic lock.

11. An electronic key comprising cryptographic calculation means and message or data transmission means for implementing a protocol according to any of claims 1 to 10 for controlling access to an electronic lock by said electronic key, characterised in that, in addition to a central processor unit, said cryptographic calculation means include at least:

- a protected access memory area for storing at least one signature value of a validity time period allocated to said electronic key and a signature or signature verification key, and

- a read-only memory used to call programs for calculating the signature value of a random variable message delivered by said electronic lock and for signature verification on the basis of said signature keys, respectively signature verification keys.

12. An electronic lock comprising cryptographic calculation means and message or data transmission means for implementing a protocol according to any of claims 1 to 10 for controlling access to said electronic lock by an electronic key, characterised in that, in addition to a central processor unit, said calculation means include at least:

- a protected access memory area for storing at least one public signature verification key, and

- a read-only memory used to call signature verification programs based on said at least one public key.

FIG.1a.

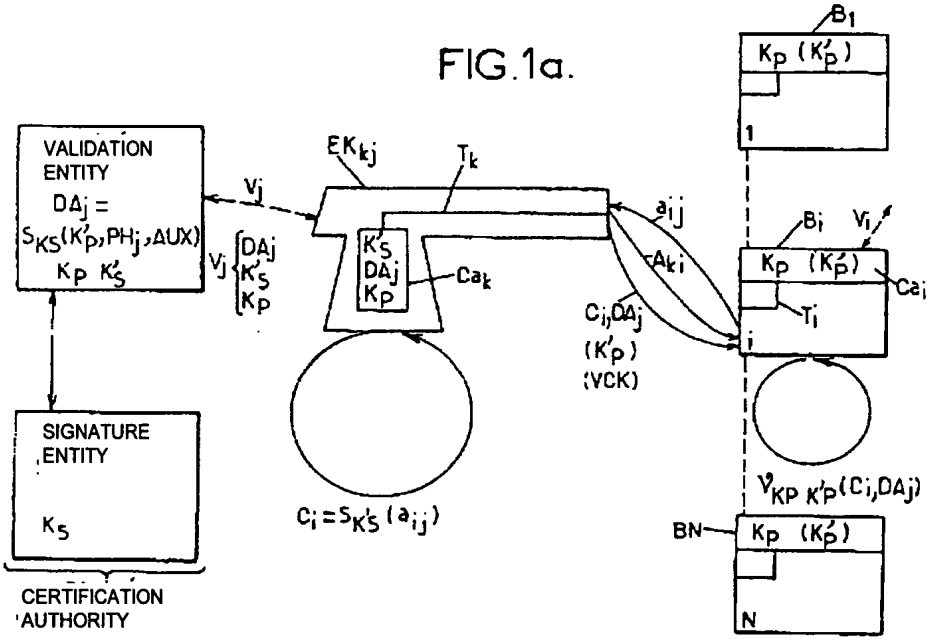

VALIDATION ENTITY
DAj =
SKS(K'P, PHj, AUX)
KP K'S
SIGNATURE ENTITY
KS
CERTIFICATION AUTHORITY
Vj
EKkj
Tk
K'S DAj KP
Cak
Ci = SK'S(aij)
aij
Aki
Ci, DAj (K'P) (VCK)
Bi Vi
KP (K'P)
Cai
Ti
i
VKP K'P(Ci, DAj)
BN
KP (K'P)
N
B1
KP (K'P)
1

FIG.1b.

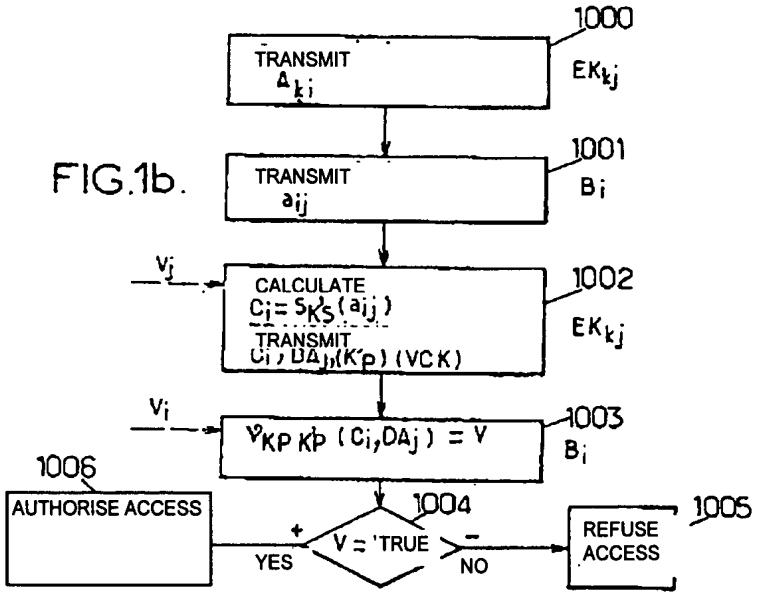

TRANSMIT Aki
1000
EKkj
TRANSMIT aij
1001
Bi
Vj
CALCULATE Ci = SK'S(aij)
TRANSMIT Ci, DAj, (K'P) (VCK)
1002
EKkj
Vi
VKP K'P (Ci, DAj) = V
1003
Bi
1006
AUTHORISE ACCESS
1004
V = 'TRUE
+
YES
-
NO
REFUSE ACCESS
1005

FIG.1c.

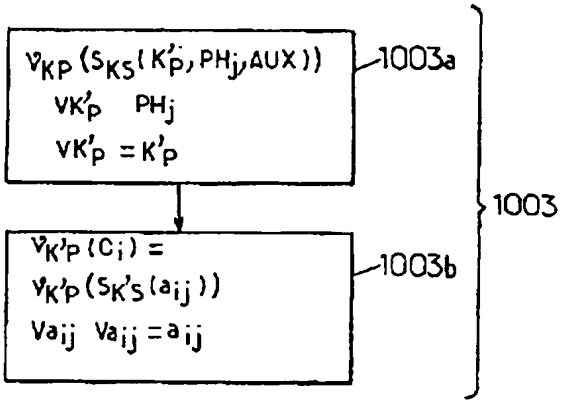


FIG.1d.

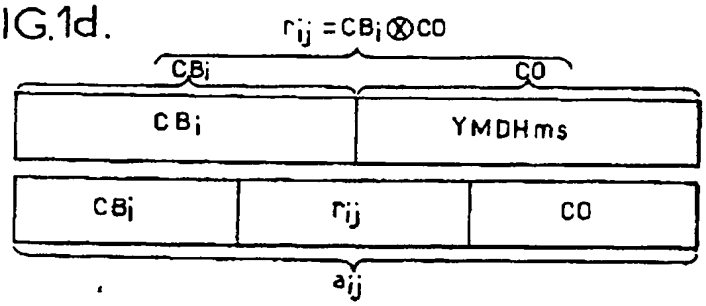
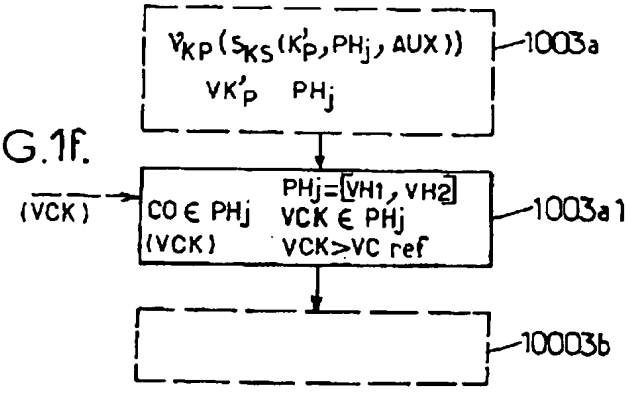


FIG.1f.



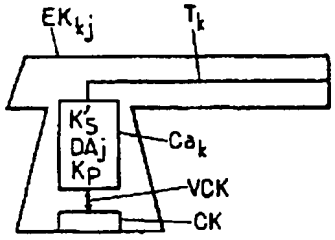

EK_kj
T_k
K'_S
DA_j
K_P
Ca_k
VCK
CK

FIG.1e.

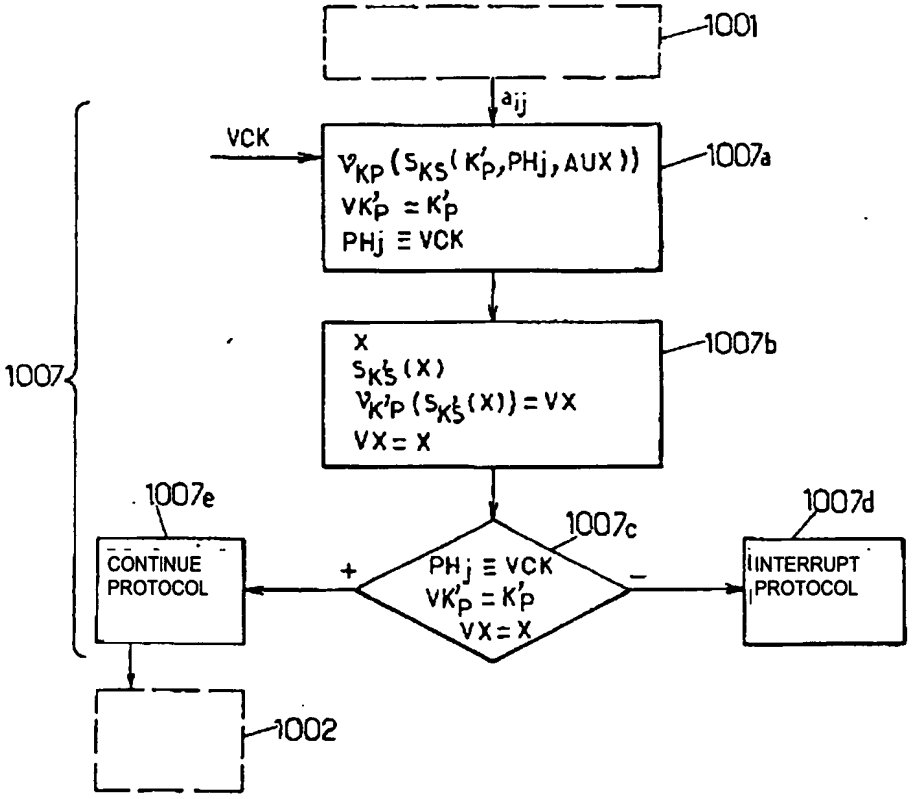

1001
a_ij
VCK
V_KP (S_KS (K'_P, PHj, AUX))
VK'_P = K'_P
PHj ≡ VCK
1007a
X
S_K'S (X)
V_K'P (S_K'S (X)) = VX
VX = X
1007b
1007
1007e
CONTINUE PROTOCOL
+
PHj ≡ VCK
VK'_P = K'_P
VX = X
1007c
−
1007d
INTERRUPT PROTOCOL
1002

FIG. 1g.

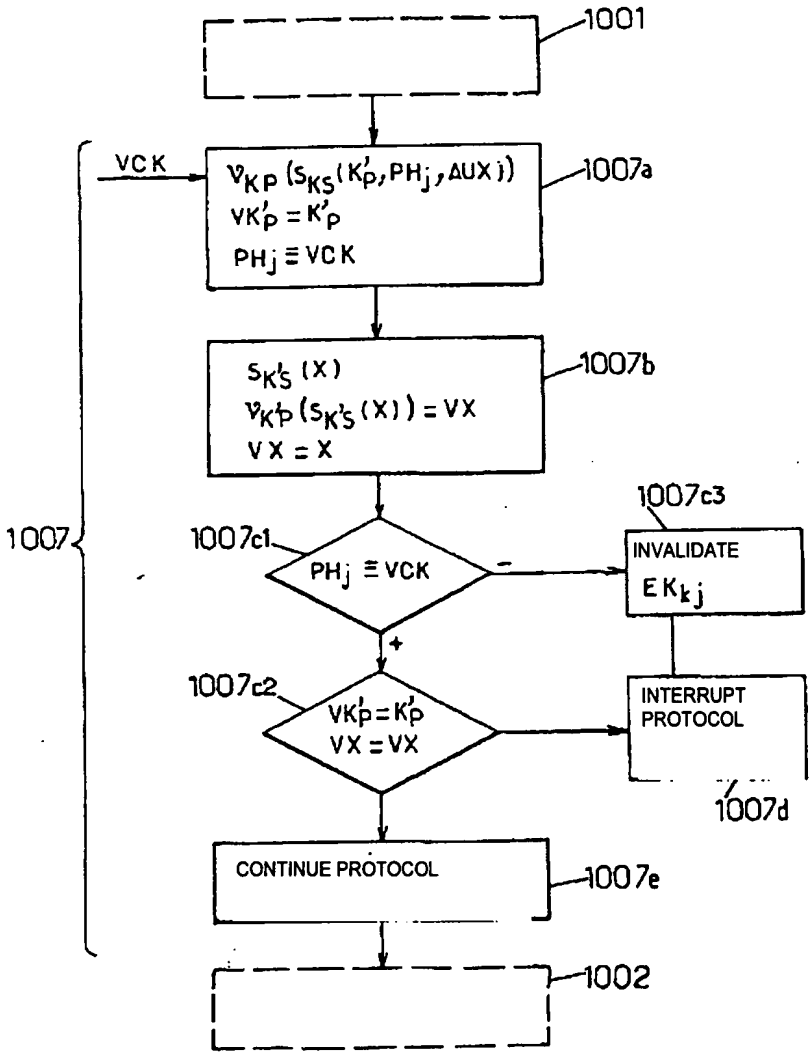

1001
VCK
$v_{KP}(s_{KS}(K'_P, PH_j, AUX))$
$VK'_P = K'_P$
$PH_j \equiv VCK$
1007a
$s_{K'S}(X)$
$v_{K'P}(s_{K'S}(X)) = VX$
$VX = X$
1007b
1007
1007c1
$PH_j \equiv VCK$
-
1007c3
INVALIDATE
EK_{kj}
+
1007c2
$VK'_P = K'_P$
$VX = VX$
INTERRUPT PROTOCOL
1007d
CONTINUE PROTOCOL
1007e
1002

FIG.2a.

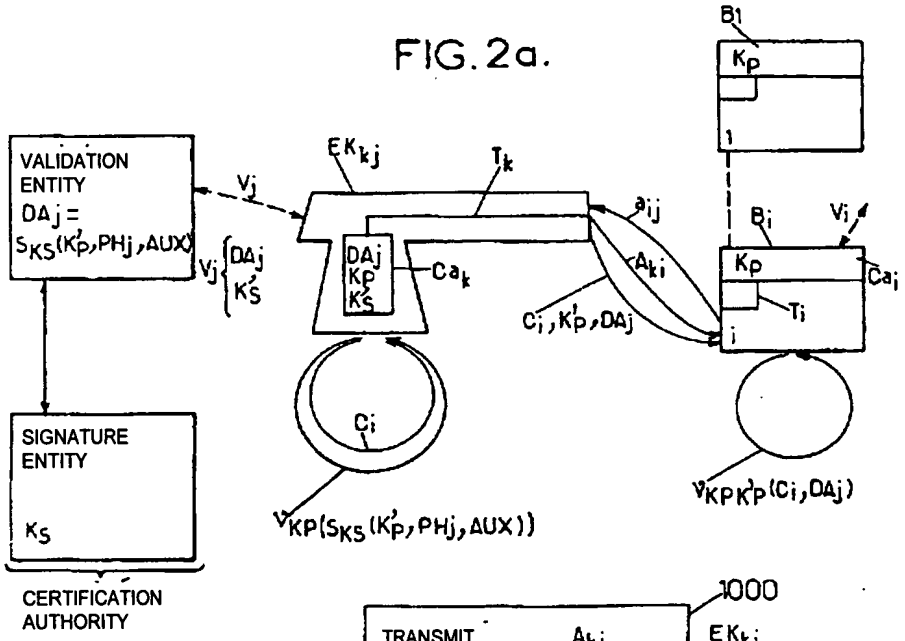

VALIDATION ENTITY
DAj = SKS(K'P, PHj, AUX)
SIGNATURE ENTITY
KS
CERTIFICATION AUTHORITY
Vj
EKkj
Tk
aij
Bi
Vi
Kp
Cak
Aki
Cai
Ti
Ci, K'p, DAj
Ci
VKP(SKS(K'P, PHj, AUX))
VKPK'P(Ci, DAj)
B1
1
i

FIG.2b.

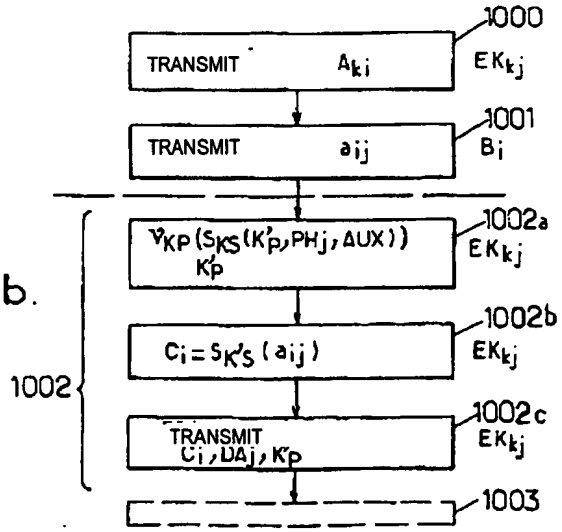
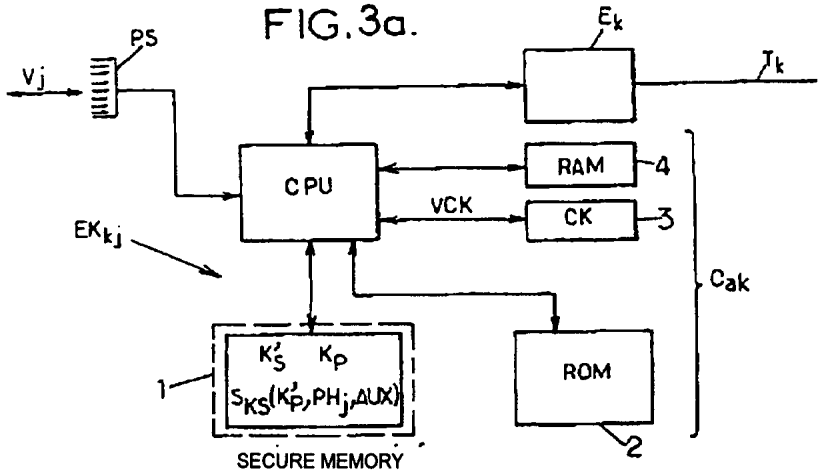

TRANSMIT Aki
EKkj
1000
TRANSMIT aij
Bi
1001
VKP(SKS(K'P, PHj, AUX))
K'P
1002a
Ci = SK'S(aij)
1002b
TRANSMIT Ci, DAj, K'P
1002c
1002
1003

FIG.3a.


PS
Vj
Ek
Tk
CPU
RAM
4
VCK
CK
3
EKkj
Cak
K's Kp
SKS(K'p,PHj,ΔUX)
1
SECURE MEMORY
ROM
2

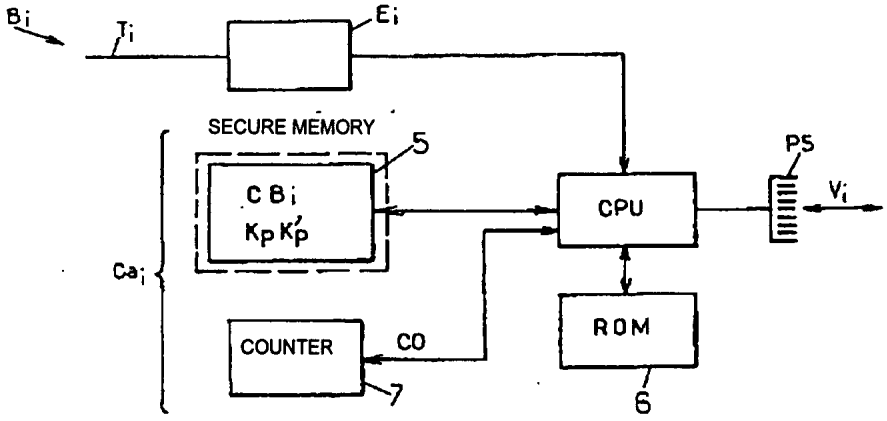

Bi
Ti
Ei
SECURE MEMORY
5
C Bi
Kp K'p
Caj
CPU
PS
Vi
COUNTER
CO
7
ROM
6

FIG.3b.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: L'ADMINISTRATION CHARGEE DE L'EXAMEN PRELIMINAIRE INTERNATIONAL

Destinataire:

FRECHEDE, M. et al.
CABINET PLASSERAUD
84, rue d'Amsterdam
F-75440 PARIS Cedex 09
FRANCE

RECU LE
12 AVR. 2000
Cbt Plasseraud

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(règle 71.1 du PCT)

	Date d'expédition *(jour/mois/année)* 10.04.00
Référence du dossier du déposant ou du mandataire BCT990009/PL	**NOTIFICATION IMPORTANTE**

Demande internationale No.	Date du dépot international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR99/00249	05/02/1999	09/02/1998

Déposant
LA POSTE et al.

1. Il est notifié au déposant que l'administration chargée de l'examen préliminaire international a établi le rapport d'examen préliminaire international pour la demande internationale et le lui transmet ci-joint, accompagné, le cas échéant, de ces annexes.

2. Une copie du présent rapport et, le cas échéant, de ses annexes est transmise au Bureau international pour communication à tous les offices élus.

3. Si tel ou tel office élu l'exige, le Bureau international établira une traduction en langue anglaise du rapport (à l'exclusion des annexes de celui-ci) et la transmettra aux offices intéressés.

4. **RAPPEL**

Pour aborder la phase nationale auprès de chaque office élu, le déposant doit accomplir certains actes (dépôt de traduction et paiement des taxes nationales) dans le délai de 30 mois à compter de la date de priorité (ou plus tard pour ce qui concerne certains offices) (article 39.1) (voir aussi le rappel envoyé par le Bureau international dans le formulaire PCT/IB/301).

Losrqu'une traduction de la demande internationale doit être remise à un office élu, elle doit comporter la traduction de toute annexe du rapport d'examen préliminaire international. Il appartient au déposant d'établir la traduction en question et de la remettre directement à chaque office élu intéressé.

Pour plus de précisions en ce qui concerne les délais applicables et les exigences des offices élus, voir le Volume II du Guide du déposant du PCT.

Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international
Office européen des brevets
D-80298 Munich
Tél. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Fonctionnaire autorisé
Garvey, R
Tél.+49 89 2399-2271

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire BCT990009/PL	**POUR SUITE A DONNER**	voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)
Demande internationale n° PCT/FR99/00249	Date du dépot international *(jour/mois/année)* 05/02/1999	Date de priorité *(jour/mois/année)* 09/02/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07C9/00		
Déposant LA POSTE et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.

 ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

 Ces annexes comprennent 9 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

 - I ☒ Base du rapport
 - II ☐ Priorité
 - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
 - IV ☐ Absence d'unité de l'invention
 - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
 - VI ☐ Certains documents cités
 - VII ☐ Irrégularités dans la demande internationale
 - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 06/09/1999	Date d'achèvement du présent rapport 10.04.00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Houillon, J-C N° de téléphone +49 89 2399 2640

Formulaire PCT/IPEA/409 (feuille de couverture) (janvier 1994)

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/00249

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1,2,4-21,23-27, 29-37	version initiale			
3,22,28	reçue(s) le	21/01/2000	avec la lettre du	19/01/2000

Revendications, N°:

1-11	reçue(s) le	21/01/2000	avec la lettre du	19/01/2000

Dessins, feuilles:

1/6-6/6	version initiale

2. Les modifications ont entrainé l'annulation :

 ☐ de la description, pages :
 ☐ des revendications, n^{os} :
 ☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-10
	Non :	Revendications	11
Activité inventive	Oui :	Revendications	1-10
	Non :	Revendications	11
Possibilité d'application industrielle	Oui :	Revendications	1-11
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Concernant le point V
Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'objet des revendications 1-10 est nouveau et implique une activité inventive car aucun des documents cités ne décrit ou suggère l'utilisation d'une cryptographie à clé publique pour l'authentification de la clé par la serrure. Les documents EP-A-807911 et EP-A-727894 utilisent respectivement dans ce cas une clé aléatoire secrète de session ou une clé secrète de communication entre l'autorité et l'utilisateur. La double utilisation de systèmes cryptographique à clé publique représente une sécurité accrue.

La revendication 11 est une revendication indépendante puisque son objet est différent de celui des autres revendications indépendantes. Elle indique bien qu'elle comprend des moyens cryptographiques et de transmission pour la mise en oeuvre du protocole selon l'une des revendications 1 à 17, mais n'indique pas dans le préambule la nature exacte de ces moyens. En effet, la simple indication de moyens permettant la mise en oeuvre d'un protocole faisant l'objet d'une revendication indépendante d'une autre catégorie n'apporte aucune limitation quant à ces moyens.
La revendication 11 précise cependant dans la partie caractérisante que ces moyens comprennent une zone mémoire mémorisant une clé publique et une mémoire comprenant le programme permettant une vérification de signature.
Toutefois, ces moyens sont déjà connus du document FR-A-2722596.
L'objet de la revendication 11 n'est donc pas nouveau.

variabilité ou de diversité du dialogue de contrôle d'accès entre la clé et la serrure électronique, au moyen d'une variable aléatoire. Une telle solution apparaît limitée en raison du fait que, d'une part, sauf à faire appel à une ou plusieurs variables physiques externes à caractère purement aléatoire, le caractère aléatoire des variables aléatoires obtenues au moyen des générateurs aléatoires ou pseudo-aléatoires usuels n'est pas totalement satisfait, alors que, d'autre part, le caractère non répétitif de la production d'un tel aléa n'est pas certain, ce qui peut ne pas décourager les fraudeurs de haute volée déterminés et disposant de ressources de calcul importantes.

En tout état de cause, les solutions précitées ne permettent donc d'inhiber avec certitude, ni une attaque par utilisation illégitime d'une clé électronique, ni une attaque par rejeu, pendant la plage horaire de validité, d'une ressource accédée.

D'autres solutions ont été proposées. La demande EP-A-727 894 décrit un système basé sur la cryptographie à clé secrète. Ces systèmes posent un problème de gestion des clés, les certificats de clé ne pouvant être facilement utilisés. La demande de brevet EP-A-807 911 décrit un système basé sur la cryptographie à clé secrète et à clé publique, utilisant des techniques de chiffrement. Un certificat de clé publique est envoyé chiffré au moyen d'une clé secrète. La clé secrète utilisée est elle-même envoyée chiffrée avec la clé publique du destinataire.

La présente invention a pour objet de remédier aux inconvénients précités des solutions préconisées par l'art antérieur.

Un tel objet est notamment atteint par l'intégration au dialogue d'accès logique, entre une ressource accédante et au moins une ressource accédée, d'un processus d'authentification de la ressource accédante par la ressource accédée, l'autorisation ou le refus de l'accès étant rendu conditionnel au succès du processus d'authentification.

Un autre objet de la présente invention est en conséquence la mise en œuvre d'un protocole de contrôle d'accès entre une ressource accédante, constituée par une

la deuxième clé publique VK'_P à la valeur de la deuxième clé publique mémorisée K'_P.

Sur réponse positive au critère de comparaison précité effectué à l'étape 1003a, une deuxième vérification est effectuée par la serrure électronique B_i à l'étape 1003b. Cette deuxième vérification, ainsi que représenté sur la figure précitée, consiste à effectuer une vérification de la valeur de signature du message variable aléatoire d'incitation à authentification.

Cette deuxième vérification est notée, compte tenu des convention précédentes :

- $\mathcal{V}_{K'P}(C_i) = \mathcal{V}_{K'P}(S_{K'S}(a_{ij}))$.

On comprend qu'au cours de cette deuxième étape de vérification réalisée à l'étape 1003b, on obtient ainsi une valeur vérifiée du message variable aléatoire d'incitation à authentification, valeur vérifiée Va_{ij}. Cette valeur vérifiée du message variable aléatoire d'incitation à authentification peut alors être comparée à la valeur du message variable aléatoire d'incitation à authentification a_{ij}, lequel aura bien entendu été mémorisé préalablement au niveau des circuits mémoires de la serrure électronique B_i.

Ainsi, on comprend que la deuxième vérification de la valeur de signature est effectuée conditionnellement à la vérification de la deuxième clé publique K'_P associée à la clé privée de signature K'_S , et donc en définitive en fonction des données spécifiques d'authentification DA_j précitées.

D'une manière générale, on indique que la première vérification représentée à l'étape 1003a de la figure 1c de l'authenticité des données spécifiques d'authentification, peut consister à contrôler la plage de validité PH_j

que B_i de l'authenticité de la valeur de signature, étape 1003 sur la figure 1a, et de manière plus particulière, étapes 1003a et 1003b de la figure 1c, suite à la première étape de vérification 1003a de l'authenticité des données spécifiques d'authentification DA_j, consistant à contrôler la plage de validité associée à la deuxième clé publique K'_P mais préalablement à la deuxième étape de vérification 1003b représentée en figure 1c, une pluralité de tests représentés en $1003a_1$, figure 1f, peut être prévue, de façon à limiter toute attaque hors de la plage de validité horaire précitée. Sur la figure 1f, la pluralité de tests est représentée de manière non limitative en une comparaison de la valeur de comptage CO délivrée par la serrure électronique B_i ou, le cas échéant, d'un signal horaire délivré par une horloge lorsque la serrure électronique est munie d'une horloge, dans la plage de validité horaire précitée. De manière plus spécifique, ce test peut consister à comparer la valeur de comptage CO aux valeurs limites définissant la plage de validité horaire PH_j précitée par exemple. En cas de non-appartenance de la variable de comptage CO ou du signal horaire correspondant à la plage de validité horaire, toute tentative d'accès est refusée par la serrure électronique B_i. D'autres tests limitant l'attaque hors de la plage de validité peuvent être envisagés.

Pour ce qui concerne la mise en œuvre de tests visant à limiter toute attaque hors d'une plage horaire PH_j déterminée, un mode de mise en œuvre préférentiel non limitatif sera décrit ci-après, dans le cas où la clé électronique est munie d'une horloge temps réel. Lors de toute tentative d'accès, les étapes de vérification telles que

REVENDICATIONS

1 Protocole de contrôle d'accès entre une clé électronique (EK_{kj}) et une serrure électronique (B_i) opérant ce contrôle d'accès, dans lequel, suite à la mise en présence de ladite clé électronique (EK_{kj}) et de ladite serrure électronique (B_i), une transmission de ladite serrure électronique à ladite clé électronique d'un message (a_{ij}) variable aléatoire d'incitation à authentification de cette clé électronique (EK_{kj}) est effectuée, caractérisé en ce que, sur réception dudit message (a_{ij}) variable aléatoire d'incitation à authentification, celui-ci consiste au moins successivement en :

- un calcul et une transmission, de ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i), d'une valeur de signature numérique dudit message variable aléatoire d'incitation à authentification à partir d'une clé privée de signature (K'_s) et de données spécifiques d'authentification (DA_j), lesdites données spécifiques d'authentification transmises par ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i) consistant au moins en un certificat de clé publique (K'_p) associée à ladite clé privée de signature (K'_s), ledit certificat de clé publique consistant en une valeur de signature numérique d'au moins une plage de validité (PH_j) relative à un droit d'accès, et de ladite clé publique (K'_p), ladite valeur de signature étant calculée au moyen d'une autre clé privée de signature (K_s) à laquelle est associée une autre clé publique (K_p) et, suite à la réception par ladite serrure électronique de ladite valeur de signature (C_i) et desdites données spécifiques d'authentification (DA_j),

- une vérification (1003) $V_{KPK'P}((C_i, DA_j))$, par ladite serrure électronique (B_i), de l'authenticité de ladite valeur de signature (C_i), en fonction desdites données spécifiques d'authentification (DA_j), et, sur réponse positive ou négative de ladite vérification,

- acceptation, respectivement refus, dudit accès.

2. Protocole selon la revendication 1, caractérisé en ce que ladite étape de vérification, par ladite serrure électronique, de ladite valeur de signature, comporte successivement :

- une première vérification (1003a), par ladite serrure électronique (B_i) de l'authenticité desdites données spécifiques d'authentification sur critère de comparaison à des données de référence, et, sur réponse positive audit critère de comparaison,

- une deuxième vérification (1003b), par ladite serrure électronique (B_i) de ladite valeur de signature (C_i), en fonction desdites données spécifiques d'authentification (DA_j).

3. Protocole selon les revendications 1 et 2, caractérisé en ce que ladite première étape de vérification par ladite serrure électronique de l'authenticité desdites données spécifiques d'authentification (DA_j) consiste à contrôler ladite plage de validité (PH_j) associée à ladite clé publique (K'_p).

4. Protocole selon la revendication 2, caractérisé en ce que la plage de validité (PH_j) comprend plusieurs intervalles temporels disjoints.

5. Protocole selon la revendication 2 ou 3, caractérisé en ce que chaque plage de validité (PH_j) consiste en au moins un intervalle temporel comportant deux bornes

exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

6. Protocole selon l'une des revendications précédentes, caractérisé en ce que ledit message (a_{ij}) variable aléatoire d'incitation à authentification est fonction d'une valeur d'identification (CB_i) de ladite serrure électronique (B_i) et d'une valeur variable (CO) continûment croissante.

7. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que, suite à la réception dudit message (a_{ij}) variable aléatoire d'incitation à authentification par ladite clé électronique (EK_{kj}) mais préalablement à l'étape de calcul et de transmission par ladite clé électronique d'une valeur de signature (C_i), ladite clé électronique (EK_{kj}) étant munie d'une horloge interne, ledit protocole consiste en outre, en une étape (1007) de vérification auxiliaire d'autorisation de calcul de signature dudit message variable aléatoire d'incitation à authentification, ladite étape de vérification (1007) auxiliaire consistant à :

- vérifier (1007a), au moyen de l'autre clé publique (K_p) associée à ladite autre clé privée de signature (K_s), ledit certificat de clé publique (K'_p) et ladite plage de validité (PH_j) associée à cette clé publique (K'_p), vis-à-vis de ladite horloge interne, ladite vérification permettant en fait de vérifier la validité de ladite clé publique (K'_p) ;

- vérifier (1007b) l'association de ladite clé privée de signature (K'_s) à ladite clé publique (K'_p), dont la validité a été vérifiée à l'étape précédente, et,

sur critère (1007c) de réponse positive et négative aux deux étapes de vérification précédentes,

- poursuivre (1007e), respectivement interrompre (1007d), ledit protocole de contrôle d'accès.

8. Protocole selon l'une des revendications 2 à 7, caractérisé en ce que, au cours de ladite étape (1003) de vérification par ladite serrure électronique (B_i) de l'authenticité de ladite valeur de signature (C_i), suite à ladite première étape (1003a) de vérification par cette serrure électronique (B_i) de l'authenticité des données spécifiques d'authentification (DA_j) consistant à contrôler ladite plage de validité (PH_j) associée à ladite clé publique (K'_P) mais préalablement à ladite étape (1003b) de deuxième vérification par cette serrure électronique (B_i) de l'authenticité de ladite valeur de signature, ledit protocole comprend en outre une pluralité de tests ($1003a_1$) limitant toute attaque hors de ladite plage de validité (PH_j).

9. Protocole selon l'une des revendications 1 à 8, caractérisé en ce que préalablement à ladite étape de calcul et de transmission de ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i) d'une valeur de signature (C_i) dudit message (a_{ij}) variable aléatoire d'incitation à authentification et de données spécifiques d'authentification (DA_j), ladite clé électronique (EK_{kj}) étant munie d'une horloge temps réel, ledit protocole comprend :

- une étape ($1007c_1$) de contrôle d'appartenance d'une variable temporelle délivrée par ladite horloge temps réel vis-à-vis de ladite plage de validité (PH_j), et, sur réponse négative à ladite étape de contrôle d'appartenance,

- une étape ($1007c_3$) d'invalidation de ladite clé électronique interrompant ledit contrôle d'accès et entraînant le refus dudit accès par ladite serrure électronique.

10. Clé électronique comprenant des moyens (C_{ak}) de calcul cryptographique et des moyens (T_k) de transmission de messages ou de données pour la mise en œuvre du protocole de contrôle d'accès à une serrure électronique (B_i) par cette clé électronique (EK_{kj}) selon l'une des revendications 1 à 9, caractérisée en ce que, outre une unité centrale de calcul (CPU), lesdits moyens (C_{ak}) de calcul cryptographique comportent au moins :

- une zone mémoire (1) à accès protégé, permettant la mémorisation d'au moins une clé privée de signature (K'_S) et de données spécifiques d'authentification (DA_j), ces données spécifiques d'authentification (DA_j) consistant au moins en un certificat de clé publique (K'_P) constitué par une valeur de signature numérique d'au moins une plage de validité (PH_j) relative à un droit d'accès, et de ladite clé publique (K'_P);

- une mémoire (4) accessible en lecture, permettant l'appel de programmes de calcul de la valeur de signature numérique d'un message variable aléatoire (a_{ij}), délivré par cette serrure électronique (B_i), au moyen de ladite clé privée de signature (K'_S).

11. Serrure électronique comprenant des moyens (C_{ai}) de calcul cryptographique et des moyens (T_i) de transmission de messages ou de données pour la mise en œuvre du protocole de contrôle d'accès à cette serrure électronique par une clé électronique (EK_{kj}), selon l'une des revendications 1 à 9, caractérisée en ce que, outre une

unité centrale de calcul (CPU), lesdits moyens (C_{ai}) de calcul comportent au moins :

- une zone mémoire (5) à accès protégé, permettant la mémorisation d'au moins une clé publique (K_P)de vérification de signature ;

- une mémoire (6) accessible en lecture, permettant l'appel de programmes de vérification de signature à partir de ladite au moins une clé publique.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire BCT990009 MF	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 99/ 00249	Date du dépôt international *(jour/mois/année)* 05/02/1999	(Date de priorité (la plus ancienne) *(jour/mois/année)* 09/02/1998
Déposant LA POSTE et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

 a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

 [] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

 b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

 [] contenu dans la demande internationale, sous forme écrite.

 [] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

 [] remis ultérieurement à l'administration, sous forme écrite.

 [] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

 [] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

 [] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

 [] le texte est approuvé tel qu'il a été remis par le déposant.

 [X] Le texte a été établi par l'administration et a la teneur suivante:

 PROTOCOLE DE CONTROLE D'ACCES ENTRE UNE CLE ET UNE SERRURE ELECTRONIQUE

5. En ce qui concerne **l'abrégé,**

 [X] le texte est approuvé tel qu'il a été remis par le déposant

 [] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 1a

 [X] suggérée par le déposant.

 [] parce que le déposant n'a pas suggéré de figure.

 [] parce que cette figure caractérise mieux l'invention.

 [] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
[redacted]/FR 99/00249

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07C9/00 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07C G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	DE 195 27 715 A (DEUTSCHE TELEKOM MOBIL) 6 février 1997 voir abrégé; figures 1,2,4-6 voir colonne 4, ligne 58 - colonne 5, ligne 51 voir colonne 7, ligne 6 - ligne 23 voir colonne 9, ligne 20 - colonne 10, ligne 38 ---	1-3,11, 12
A	US 5 546 463 A (CAPUTO ANTHONY A ET AL) 13 août 1996 voir abrégé; figures 2,5A,5B,8 voir colonne 5, ligne 16 - ligne 67 voir colonne 6, ligne 56 - colonne 7, ligne 55 voir colonne 8, ligne 40 - colonne 10, ligne 14 --- -/--	1,7,11, 12

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
29 avril 1999	11/05/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Buron, E

1

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 427 465 A (AMERICAN TELEPHONE & TELEGRAPH) 15 mai 1991 voir abrégé; figures 1,5,7,8 voir colonne 5, ligne 1 - colonne 7, ligne 11 voir colonne 11, ligne 1 - colonne 12, ligne 24 voir colonne 13, ligne 30 - colonne 14, ligne 45	1,11,12
A	FR 2 722 596 A (FRANCE TELECOM) 19 janvier 1996 cité dans la demande voir abrégé; revendications 1-4,9,10,14; figures voir page 3, ligne 6 - page 7, ligne 31 voir page 11, ligne 20 - page 12, ligne 3	1-6,11, 12
A	GB 2 154 344 A (NAT RES DEV) 4 septembre 1985 voir abrégé; figures 1,3 voir page 4, ligne 7 - page 5, ligne 38	1,11
A	US 4 870 400 A (DOWNS STEPHEN R ET AL) 26 septembre 1989 voir abrégé; figure 7 voir colonne 9, ligne 8 - ligne 25 voir colonne 10, ligne 23 - ligne 54	3,4,6,9
A	US 5 243 175 A (KATO AKIO) 7 septembre 1993 voir abrégé; figures 1-3 voir colonne 1, ligne 9 - colonne 3, ligne 15 voir colonne 3, ligne 62 - colonne 5, ligne 61 voir colonne 7, ligne 67 - colonne 8, ligne 14	8,10
A	US 5 130 519 A (BUSH GEORGE ET AL) 14 juillet 1992 voir abrégé; figure 3 voir colonne 4, ligne 44 - ligne 50	7

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 99/00249

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 19527715	A	06-02-1997	NONE		
US 5546463	A	13-08-1996	US	5878142 A	02-03-1999
			US	5778071 A	07-07-1998
EP 0427465	A	15-05-1991	US	5120939 A	09-06-1992
			CA	2023872 A,C	10-05-1991
			DE	69016589 D	16-03-1995
			DE	69016589 T	07-09-1995
			JP	1921556 C	07-04-1995
			JP	3158955 A	08-07-1991
			JP	6052518 B	06-07-1994
FR 2722596	A	19-01-1996	AT	175796 T	15-01-1999
			AU	2931795 A	16-02-1996
			CA	2171626 A	01-02-1996
			DE	69507278 D	25-02-1999
			EP	0719438 A	03-07-1996
			WO	9602899 A	01-02-1996
			JP	9503089 T	25-03-1997
			US	5768379 A	16-06-1998
GB 2154344	A	04-09-1985	US	4799258 A	17-01-1989
US 4870400	A	26-09-1989	NONE		
US 5243175	A	07-09-1993	JP	1259483 A	17-10-1989
US 5130519	A	14-07-1992	US	5265162 A	23-11-1993

4
+

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 13 APR 2000
WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire BCT990009/PL	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/00249	Date du dépot international *(jour/mois/année)* 05/02/1999	Date de priorité *(jour/mois/année)* 09/02/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07C9/00		
Déposant LA POSTE et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 4 feuilles, y compris la présente feuille de couverture.

 ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

 Ces annexes comprennent 9 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

 - I ☒ Base du rapport
 - II ☐ Priorité
 - III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
 - IV ☐ Absence d'unité de l'invention
 - V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
 - VI ☐ Certains documents cités
 - VII ☐ Irrégularités dans la demande internationale
 - VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 06/09/1999	Date d'achèvement du présent rapport 10.04.00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Houillon, J-C N° de téléphone +49 89 2399 2640

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR99/00249

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1,2,4-21,23-27, 29-37	version initiale			
3,22,28	reçue(s) le	21/01/2000	avec la lettre du	19/01/2000

Revendications, N°:

1-11	reçue(s) le	21/01/2000	avec la lettre du	19/01/2000

Dessins, feuilles:

1/6-6/6	version initiale

2. Les modifications ont entrainé l'annulation :

 ☐ de la description, pages :
 ☐ des revendications, n^{os} :
 ☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-10
	Non :	Revendications	11
Activité inventive	Oui :	Revendications	1-10
	Non :	Revendications	11
Possibilité d'application industrielle	Oui :	Revendications	1-11
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Concernant le point V

Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

L'objet des revendications 1-10 est nouveau et implique une activité inventive car aucun des documents cités ne décrit ou suggère l'utilisation d'une cryptographie à clé publique pour l'authentification de la clé par la serrure. Les documents EP-A-807911 et EP-A-727894 utilisent respectivement dans ce cas une clé aléatoire secrète de session ou une clé secrète de communication entre l'autorité et l'utilisateur. La double utilisation de systèmes cryptographique à clé publique représente une sécurité accrue.

La revendication 11 est une revendication indépendante puisque son objet est différent de celui des autres revendications indépendantes. Elle indique bien qu'elle comprend des moyens cryptographiques et de transmission pour la mise en oeuvre du protocole selon l'une des revendications 1 à 17, mais n'indique pas dans le préambule la nature exacte de ces moyens. En effet, la simple indication de moyens permettant la mise en oeuvre d'un protocole faisant l'objet d'une revendication indépendante d'une autre catégorie n'apporte aucune limitation quant à ces moyens.
La revendication 11 précise cependant dans la partie caractérisante que ces moyens comprennent une zone mémoire mémorisant une clé publique et une mémoire comprenant le programme permettant une vérification de signature.
Toutefois, ces moyens sont déjà connus du document FR-A-2722596.
L'objet de la revendication 11 n'est donc pas nouveau.

variabilité ou de diversité du dialogue de contrôle d'accès entre la clé et la serrure électronique, au moyen d'une variable aléatoire. Une telle solution apparaît limitée en raison du fait que, d'une part, sauf à faire appel à une ou plusieurs variables physiques externes à caractère purement aléatoire, le caractère aléatoire des variables aléatoires obtenues au moyen des générateurs aléatoires ou pseudo-aléatoires usuels n'est pas totalement satisfait, alors que, d'autre part, le caractère non répétitif de la production d'un tel aléa n'est pas certain, ce qui peut ne pas décourager les fraudeurs de haute volée déterminés et disposant de ressources de calcul importantes.

En tout état de cause, les solutions précitées ne permettent donc d'inhiber avec certitude, ni une attaque par utilisation illégitime d'une clé électronique, ni une attaque par rejeu, pendant la plage horaire de validité, d'une ressource accédée.

D'autres solutions ont été proposées. La demande EP-A-727 894 décrit un système basé sur la cryptographie à clé secrète. Ces systèmes posent un problème de gestion des clés, les certificats de clé ne pouvant être facilement utilisés. La demande de brevet EP-A-807 911 décrit un système basé sur la cryptographie à clé secrète et à clé publique, utilisant des techniques de chiffrement. Un certificat de clé publique est envoyé chiffré au moyen d'une clé secrète. La clé secrète utilisée est elle-même envoyée chiffrée avec la clé publique du destinataire.

La présente invention a pour objet de remédier aux inconvénients précités des solutions préconisées par l'art antérieur.

Un tel objet est notamment atteint par l'intégration au dialogue d'accès logique, entre une ressource accédante et au moins une ressource accédée, d'un processus d'authentification de la ressource accédante par la ressource accédée, l'autorisation ou le refus de l'accès étant rendu conditionnel au succès du processus d'authentification.

Un autre objet de la présente invention est en conséquence la mise en œuvre d'un protocole de contrôle d'accès entre une ressource accédante, constituée par une

la deuxième clé publique VK'_P à la valeur de la deuxième clé publique mémorisée K'_P.

Sur réponse positive au critère de comparaison précité effectué à l'étape 1003a, une deuxième vérification est effectuée par la serrure électronique B_i à l'étape 1003b. Cette deuxième vérification, ainsi que représenté sur la figure précitée, consiste à effectuer une vérification de la valeur de signature du message variable aléatoire d'incitation à authentification.

Cette deuxième vérification est notée, compte tenu des convention précédentes :

- $\mathcal{V}_{K'P}(C_i) = \mathcal{V}_{K'P}(S_{K'S}(a_{ij}))$.

On comprend qu'au cours de cette deuxième étape de vérification réalisée à l'étape 1003b, on obtient ainsi une valeur vérifiée du message variable aléatoire d'incitation à authentification, valeur vérifiée Va_{ij}. Cette valeur vérifiée du message variable aléatoire d'incitation à authentification peut alors être comparée à la valeur du message variable aléatoire d'incitation à authentification a_{ij}, lequel aura bien entendu été mémorisé préalablement au niveau des circuits mémoires de la serrure électronique B_i.

Ainsi, on comprend que la deuxième vérification de la valeur de signature est effectuée conditionnellement à la vérification de la deuxième clé publique K'_P associée à la clé privée de signature K'_S , et donc en définitive en fonction des données spécifiques d'authentification DA_j précitées.

D'une manière générale, on indique que la première vérification représentée à l'étape 1003a de la figure 1c de l'authenticité des données spécifiques d'authentification, peut consister à contrôler la plage de validité PH_j

que B_i de l'authenticité de la valeur de signature, étape 1003 sur la figure 1a, et de manière plus particulière, étapes 1003a et 1003b de la figure 1c, suite à la première étape de vérification 1003a de l'authenticité des données spécifiques d'authentification DA_j, consistant à contrôler la plage de validité associée à la deuxième clé publique K'_P mais préalablement à la deuxième étape de vérification 1003b représentée en figure 1c, une pluralité de tests représentés en $1003a_1$, figure 1f, peut être prévue, de façon à limiter toute attaque hors de la plage de validité horaire précitée. Sur la figure 1f, la pluralité de tests est représentée de manière non limitative en une comparaison de la valeur de comptage CO délivrée par la serrure électronique B_i ou, le cas échéant, d'un signal horaire délivré par une horloge lorsque la serrure électronique est munie d'une horloge, dans la plage de validité horaire précitée. De manière plus spécifique, ce test peut consister à comparer la valeur de comptage CO aux valeurs limites définissant la plage de validité horaire PH_j précitée par exemple. En cas de non-appartenance de la variable de comptage CO ou du signal horaire correspondant à la plage de validité horaire, toute tentative d'accès est refusée par la serrure électronique B_i. D'autres tests limitant l'attaque hors de la plage de validité peuvent être envisagés.

Pour ce qui concerne la mise en œuvre de tests visant à limiter toute attaque hors d'une plage horaire PH_j déterminée, un mode de mise en œuvre préférentiel non limitatif sera décrit ci-après, dans le cas où la clé électronique est munie d'une horloge temps réel. Lors de toute tentative d'accès, les étapes de vérification telles que

REVENDICATIONS

1 Protocole de contrôle d'accès entre une clé électronique (EK_{kj}) et une serrure électronique (B_i) opérant ce contrôle d'accès, dans lequel, suite à la mise en présence de ladite clé électronique (EK_{kj}) et de ladite serrure électronique (B_i), une transmission de ladite serrure électronique à ladite clé électronique d'un message (a_{ij}) variable aléatoire d'incitation à authentification de cette clé électronique (EK_{kj}) est effectuée, caractérisé en ce que, sur réception dudit message (a_{ij}) variable aléatoire d'incitation à authentification, celui-ci consiste au moins successivement en :

- un calcul et une transmission, de ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i), d'une valeur de signature numérique dudit message variable aléatoire d'incitation à authentification à partir d'une clé privée de signature (K'_s) et de données spécifiques d'authentification (DA_j), lesdites données spécifiques d'authentification transmises par ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i) consistant au moins en un certificat de clé publique (K'_p) associée à ladite clé privée de signature (K'_s), ledit certificat de clé publique consistant en une valeur de signature numérique d'au moins une plage de validité (PH_j) relative à un droit d'accès, et de ladite clé publique (K'_p), ladite valeur de signature étant calculée au moyen d'une autre clé privée de signature (K_s) à laquelle est associée une autre clé publique (K_p) et, suite à la réception par ladite serrure électronique de ladite valeur de signature (C_i) et desdites données spécifiques d'authentification (DA_j),

- une vérification (1003) $V_{KPK'P}((C_i,DA_j))$, par ladite serrure électronique (B_i), de l'authenticité de ladite valeur de signature (C_i), en fonction desdites données spécifiques d'authentification (DA_j), et, sur réponse positive ou négative de ladite vérification,

- acceptation, respectivement refus, dudit accès.

2. Protocole selon la revendication 1, caractérisé en ce que ladite étape de vérification, par ladite serrure électronique, de ladite valeur de signature, comporte successivement :

- une première vérification (1003a), par ladite serrure électronique (B_i) de l'authenticité desdites données spécifiques d'authentification sur critère de comparaison à des données de référence, et, sur réponse positive audit critère de comparaison,

- une deuxième vérification (1003b), par ladite serrure électronique (B_i) de ladite valeur de signature (C_i), en fonction desdites données spécifiques d'authentification (DA_j).

3. Protocole selon les revendications 1 et 2, caractérisé en ce que ladite première étape de vérification par ladite serrure électronique de l'authenticité desdites données spécifiques d'authentification (DA_j) consiste à contrôler ladite plage de validité (PH_j) associée à ladite clé publique (K'_p).

4. Protocole selon la revendication 2, caractérisé en ce que la plage de validité (PH_j) comprend plusieurs intervalles temporels disjoints.

5. Protocole selon la revendication 2 ou 3, caractérisé en ce que chaque plage de validité (PH_j) consiste en au moins un intervalle temporel comportant deux bornes

exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

6. Protocole selon l'une des revendications précédentes, caractérisé en ce que ledit message (a_{ij}) variable aléatoire d'incitation à authentification est fonction d'une valeur d'identification (CB_i) de ladite serrure électronique (B_i) et d'une valeur variable (CO) continûment croissante.

7. Protocole selon l'une des revendications 1 à 6, caractérisé en ce que, suite à la réception dudit message (a_{ij}) variable aléatoire d'incitation à authentification par ladite clé électronique (EK_{kj}) mais préalablement à l'étape de calcul et de transmission par ladite clé électronique d'une valeur de signature (C_i), ladite clé électronique (EK_{kj}) étant munie d'une horloge interne, ledit protocole consiste en outre, en une étape (1007) de vérification auxiliaire d'autorisation de calcul de signature dudit message variable aléatoire d'incitation à authentification, ladite étape de vérification (1007) auxiliaire consistant à :

- vérifier (1007a), au moyen de l'autre clé publique (K_p) associée à ladite autre clé privée de signature (K_s), ledit certificat de clé publique (K'_p) et ladite plage de validité (PH_j) associée à cette clé publique (K'_p), vis-à-vis de ladite horloge interne, ladite vérification permettant en fait de vérifier la validité de ladite clé publique (K'_p) ;

- vérifier (1007b) l'association de ladite clé privée de signature (K'_s) à ladite clé publique (K'_p), dont la validité a été vérifiée à l'étape précédente, et,

sur critère (1007c) de réponse positive et négative aux deux étapes de vérification précédentes,

- poursuivre (1007e), respectivement interrompre (1007d), ledit protocole de contrôle d'accès.

8. Protocole selon l'une des revendications 2 à 7, caractérisé en ce que, au cours de ladite étape (1003) de vérification par ladite serrure électronique (B_i) de l'authenticité de ladite valeur de signature (C_i), suite à ladite première étape (1003a) de vérification par cette serrure électronique (B_i) de l'authenticité des données spécifiques d'authentification (DA_j) consistant à contrôler ladite plage de validité (PH_j) associée à ladite clé publique (K'_P) mais préalablement à ladite étape (1003b) de deuxième vérification par cette serrure électronique (B_i) de l'authenticité de ladite valeur de signature, ledit protocole comprend en outre une pluralité de tests ($1003a_1$) limitant toute attaque hors de ladite plage de validité (PH_j).

9. Protocole selon l'une des revendications 1 à 8, caractérisé en ce que préalablement à ladite étape de calcul et de transmission de ladite clé électronique (EK_{kj}) à ladite serrure électronique (B_i) d'une valeur de signature (C_i) dudit message (a_{ij}) variable aléatoire d'incitation à authentification et de données spécifiques d'authentification (DA_j), ladite clé électronique (EK_{kj}) étant munie d'une horloge temps réel, ledit protocole comprend :

- une étape ($1007c_1$) de contrôle d'appartenance d'une variable temporelle délivrée par ladite horloge temps réel vis-à-vis de ladite plage de validité (PH_j), et, sur réponse négative à ladite étape de contrôle d'appartenance,

- une étape ($1007c_3$) d'invalidation de ladite clé électronique interrompant ledit contrôle d'accès et entraînant le refus dudit accès par ladite serrure électronique.

10. Clé électronique comprenant des moyens (C_{ak}) de calcul cryptographique et des moyens (T_k) de transmission de messages ou de données pour la mise en œuvre du protocole de contrôle d'accès à une serrure électronique (B_i) par cette clé électronique (EK_{kj}) selon l'une des revendications 1 à 9, caractérisée en ce que, outre une unité centrale de calcul (CPU), lesdits moyens (C_{ak}) de calcul cryptographique comportent au moins :

- une zone mémoire (1) à accès protégé, permettant la mémorisation d'au moins une clé privée de signature (K'_S) et de données spécifiques d'authentification (DA_j), ces données spécifiques d'authentification (DA_j) consistant au moins en un certificat de clé publique (K'_P) constitué par une valeur de signature numérique d'au moins une plage de validité (PH_j) relative à un droit d'accès, et de ladite clé publique (K'_P);

- une mémoire (4) accessible en lecture, permettant l'appel de programmes de calcul de la valeur de signature numérique d'un message variable aléatoire (a_{ij}), délivré par cette serrure électronique (B_i), au moyen de ladite clé privée de signature (K'_S).

11. Serrure électronique comprenant des moyens (C_{ai}) de calcul cryptographique et des moyens (T_i) de transmission de messages ou de données pour la mise en œuvre du protocole de contrôle d'accès à cette serrure électronique par une clé électronique (EK_{kj}), selon l'une des revendications 1 à 9, caractérisée en ce que, outre une

FEUILLE MODIFIEE

unité centrale de calcul (CPU), lesdits moyens (C_{ai}) de calcul comportent au moins :

- une zone mémoire (5) à accès protégé, permettant la mémorisation d'au moins une clé publique (K_P) de vérification de signature ;

- une mémoire (6) accessible en lecture, permettant l'appel de programmes de vérification de signature à partir de ladite au moins une clé publique.